



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/043,910

01/11/2002

Frank Lee

TRNDP006

7252

22434

7590

01/17/2008

BEYER WEAVER LLP

P.O. BOX 70250

OAKLAND, CA 94612-0250

EXAMINER

MOORTHY, ARAVIND K

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

01/17/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/043,910

Applicant(s)

LEE ET AL.

Examiner

Aravind K. Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 October 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8, 10-17, 21-25 and 36-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8, 10-17, 21-25 and 36-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTQ-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 29 October 2007.
2. Claims 1-8, 10-17, 21-25 and 36-38 are pending in the application.
3. Claims 1-8, 10-17, 21-25 and 36-38 have been rejected.
4. Claims 9, 18-20 and 26-35 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 29 October 2007 has been entered.

Response to Arguments

6. Applicant's arguments filed 29 October 2007 have been fully considered but they are not persuasive.

On page 2, the applicant argues that Touboul does not teach a scan module or the act of scanning a protocol field and identifying a content-related protocol. The applicant argues that Touboul does not teach or show a proxy module adding a re-direction header to a request so that it goes to a proxy server as recited in claim 1. The applicant argues that Touboul does not anticipate a proxy server's content scanning module and user-defined configuration data scanning module as recited in claim 1. The applicant argues that Touboul does not teach decoding a response or scanning the decoded response as recited in claim 16. The applicant argues that Touboul does not teach processing a request using user-defined configuration data.

The applicant argues that Smithson does not teach a proxy server quarantining undesirable content as recited in claim 8.

The examiner respectfully disagrees. The applicant's specification defines the scan module as examining the protocols present in the request to determine if a request is for content, such as a request or retrieve protocol [0051]. Touboul discloses "downloadables". Touboul defines a downloadable as an executable application program, which is downloaded from a source computer and run on the destination computer. The downloadable is requested by an ongoing process such as by an Internet browser or web engine. Touboul discloses in path 2, the first comparator 320 delivers the Downloadable, the Downloadable ID and the security policy 305 to the code scanner 325. If the DSP data 310 of the received Downloadable is known, the code scanner 325 retrieves and forwards the information to the ACL comparator 330. Otherwise, the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker. Therefore, since Touboul discloses scanning the downloadable. Touboul discloses scanning the request for a content

request. Touboul discloses in path 1, the first comparator 320 checks the policy selector 405 of the security policy 305 that was received from the policy finder 317. If the policy selector 405 is either "Allowed" or "Blocked," then the first comparator 320 forwards this result directly to the logical engine 333. Otherwise, the first comparator 320 invokes the comparisons in path2 and/or path 3 and/or path 4 based on the contents of policy selector 405. It will be appreciated that the first comparator 320 itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override 425. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked." Touboul discloses that if the code scanner 325 in step 71 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725. Touboul discloses that the security policy editor 505 uses an I/O interface for enabling a authorized user modification of the security policies 305. Smithson discloses switching from virus quarantining to virus deletion when a virus is detected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-7, 10-17, 19-25 and 36-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Touboul U.S. Patent No. 6,804,780 B1.

As to claim 1, Touboul discloses a system for identifying undesirable content in responses sent in reply to a user request for content, the system comprising:

a user input device that generates a request for content including an address of a target server and a protocol field [column 6, lines 52-62];

a network component that executes a redirection program, the redirecting program including a scan module that receives the user request for content and is capable of identifying the request as a request for content by scanning the protocol field and identifying a content-related protocol [column 6 line 63 to column 7 line 20], and a proxy module that modifies the request for content by adding a redirection destination header to the request so that it is redirected to a proxy server [column 7, lines 31-43];

a network that routes the request for content to the proxy server [column 7, lines 31-43]; and

the proxy server that receives user-defined configuration data during a negotiation phase of establishing a connection between the proxy module and proxy server, receives the request for content, removes the redirection header, forwards the request to the target server, and receives a response from the target server [column 7, lines 31-59], the proxy server having a content scanning module to scan the response and a user-defined configuration data scanning module to apply user-defined configuration data to the response [column 7, lines 31-59].

As to claim 2, Touboul discloses that the proxy server identifies undesirable content in the response and processes the response according to defined parameters [column 8, lines 7-20].

As to claim 3, Touboul discloses that the proxy server sends at least a portion of the response to the user, the portion of the response not including the undesirable content [column 6 line 63 to column 7 line 20].

As to claim 4, Touboul discloses that the proxy server sends a notification message back to the user, the notification message containing data related to the undesirable content [column 7, lines 44-59].

As to claim 5, Touboul discloses the system further comprising:

a user preference module that receives user-defined parameters utilized by the proxy server when processing the response [column 7, lines 31-43].

As to claims 6 and 19, Touboul discloses that the proxy module redirects the request to the proxy server by modifying the request [column 6 line 63 to column 7 line 20].

As to claims 7 and 20, Touboul discloses that the proxy module modifies the request by adding a redirection destination header to the request [column 7, lines 31-43].

As to claim 10, Touboul discloses that the defined parameters are proxy server default parameters [column 7, lines 31-43].

As to claim 11, Touboul discloses that the defined parameters are user-defined parameters [column 7, lines 31-43].

As to claim 12, Touboul discloses that the defined parameters are a combination of user-defined parameters and proxy server default parameters [column 7, lines 31-43].

As to claims 13 and 14, Touboul discloses that the scan module and the proxy module are located in a network gateway device [column 4, lines 4-22].

As to claim 15, Touboul discloses that the network gateway device further comprises a firewall and a router [column 4, lines 4-22].

As to claim 16, Touboul discloses a method for identifying undesirable content in responses sent in reply to a user request for content, the method comprising:

receiving, at a redirection program executing on a network computing device, input from a user computer including at least one request for content addressed to a target server, the request having an address of the target server and a protocol field [column 6, lines 52-62];

identifying at a scan module in the redirection program the request for content by scanning the protocol field and identifying a content-related protocol [column 6 line 63 to column 7 line 20];

at a proxy module in the redirection program, modifying the request by adding a redirection header to the request, thereby redirecting the request to a proxy server [column 6 line 63 to column 7 line 20];

receiving the request for content at the proxy server [column 6 line 63 to column 7 line 20];

receiving user-defined configuration data at the proxy server during a negotiation phase of establishing a connection between the proxy module and proxy server [column 7, lines 31-59];

removing the redirection destination header from the request at the proxy server [column 6 line 63 to column 7 line 20];

sending the request for content from the proxy server to the target server for generation of a response [column 8, lines 44-59];

receiving the response from the target server at the proxy server [column 8, lines 44-59];

decoding the response at the proxy server [column 8, lines 44-59];

scanning the decoded response for a computer virus, junk e-mail, or pornographic content at the proxy server [column 8, lines 44-59];

if a computer virus, junk e-mail or pornographic content is detected, processing the decode response at the proxy server according to the user-defined configuration data, re-encoding the response and appending a return address so that the response is sent to the user computer [column 9, lines 11-34]; and

if a computer virus, junk e-mail, or pornographic content is not detected, re-encoding the response and appending the return address so that the response is sent to the user computer [column 9, lines 11-34].

As to claim 17, Touboul discloses the method further comprising:

identifying undesirable content in the response [column 6 line 63 to column 7 line 20];

modifying the response to remove the undesirable content [column 6 line 63 to column 7 line 20]; and

sending the modified response from the proxy server to the user computer [column 6 line 63 to column 7 line 20].

As to claim 21, Touboul discloses that the request for content is redirected to the proxy server by establishing a session with the proxy server [column 6 line 63 to column 7 line 20].

As to claim 22, Touboul discloses the method further comprising:

receiving input of at least one user-defined parameter at the proxy module which stores the parameter in a database and may forward to the proxy server during negotiation phase of the connection with the proxy server [column 7, lines 31-43].

As to claims 23, Touboul discloses that the user-defined parameter is input using a browser application [column 7, lines 31-43].

As to claim 24, Touboul discloses that the user-defined parameter is sent to the proxy server by modifying the request for content [column 7, lines 31-43].

As to claim 25, Touboul discloses that the user-defined parameter is sent to the proxy server during a session established with the proxy server [column 7, lines 31-43].

As to claim 36, Touboul discloses storing the user-defined configuration data at the proxy module [column 7, lines 31-43].

As to claim 37, Touboul discloses storing the user-defined configuration data at the proxy server [column 7, lines 31-43].

As to claim 38, Touboul discloses retrieving the previously stored user-defined configuration data at the proxy server when processing the decoded response [column 7, lines 31-43].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Touboul U.S. Patent No. 6,804,780 B1 as applied to claim 1 above, and further in view of Smithson et al US 6,898,715 B1.

As to claim 8, Touboul does not teach that the proxy server further quarantines undesirable content.

Smithson et al teaches a proxy that quarantines computer virus outbreaks [column 6 line 13 to column 7 line 17].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Touboul so that the proxy server would have quarantined undesirable content it was content containing a virus.


It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Touboul by the teaching of Smithson et al because it prevents the undesirable content (i.e. virus) to spread throughout the network [column 1, lines 48-64].


Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy 
January 8, 2008


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100